WÓJT GMINY
SKOROSZYCE

ZARZĄDZENIE 299/2018
Wójta Gminy Skoroszyce
z dnia 25.05.2018 roku

w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi

Na podstawie art. 32 ust.1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

zarządza się, co następuje:

§ 1.

Wprowadza się do użytku służbowego:

1. Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Skoroszycach stanowiąca załącznik nr 1 do niniejszego zarządzenia,
2. Instrukcję zarządzania systemami informatycznymi w Urzędzie Gminy w Skoroszycach stanowiąca załącznik nr 2 do niniejszego zarządzenia.

§ 2.

Zobowiązuje się wszystkich pracowników Urzędu Gminy w Skoroszycach do zapoznania się z treścią niniejszego zarządzenia.

§ 3.

Oświadcza się, że wszystkie załączniki załączone do niniejszego zarządzenia zawierają informacje prawnie chronione.

§ 4.

Traci moc zarządzenie Nr 8/2015 Wójta Gminy Skoroszyce z dnia 1 października 2015r. w sprawie dokumentacji opisującej sposób przetwarzania danych osobowych.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
B. Dybczak
mgr inż. Barbara Dybczak

POLITYKA BEZPIECZEŃSTWA

Urząd Gminy w Skoroszycach

Spis treści

1. WSTĘP

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka Bezpieczeństwa została opracowana zgodnie z wymogami określonymi w § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024.)

Jako załącznik do niniejszej Polityki Bezpieczeństwa opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją Zarządzania Systemem Informatycznym". Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: **Dz. U. 2016 r. poz. 922 ze zm.**),
oraz aktów wykonawczych wydanych na podstawie ww. ustawy.

- rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (rozporządzenie PEiRUE), dalej zwanym „rozporządzeniem RODO"

-

2. DEFINICJE

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1. Polityka – rozumie się przez to Politykę Bezpieczeństwa ochrony danych osobowych.
2. Administrator Danych Osobowych (ADO) – decydujący o celach i środkach przetwarzania danych osobowych.
3. Inspektor Ochrony Danych Osobowych (IODO) – pracownik wyznaczony przez ADO bądź osoba działająca na podstawie odrębnej umowy, odpowiedzialna za organizację ochrony danych osobowych.
4. Ustawa – rozumie się przez to ustawę z dnia 29.sierpnia.1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922 ze zm.).
5. Rozporządzenie – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
6. Rozporządzenie PEiRUE - rozumie się rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
7. Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.„dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
8. profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
9. „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
10. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów.„zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

11. dostęp do danych – prawo określone w art. 15 ogólnego rozporządzenia RODO; sprostowanie danych - prawo określone w art. 16 ogólnego rozporządzenia RODO; usunięcie danych – prawo do bycia zapomnianym - prawo określone w art. 17 ogólnego rozporządzenia RODO; ograniczenie przetwarzania - prawo określone w art. 18 ogólnego rozporządzenia RODO; przenoszenie danych - prawo określone w art. 20 ogólnego rozporządzenia RODO;

12. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.;

13. Zgoda osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

14. Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe.

15. Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie.

16. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

17. Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.

18. Użytkownik - pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych.

19. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

20. Nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. taśmy, pen drive, CD-DVD Rom, dyski twarde.

Pojęcia i sformułowania nie zdefiniowane w niniejszej Polityce Bezpieczeństwa należy interpretować zgodnie z Rozporządzeniem RODO

3. ZAKRES UPRAWNIEŃ/ZADAŃ IODO

Zakres uprawnień/zadań IODO został przedstawiony w załączniku do zarządzeniu o powołaniu IODO. Powołane Inspektora Ochrony Danych Osobowych nastąpiło poprzez Zarządzeniem z dnia 25.05.2018r.

4. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, wzór wykazu stanowi załącznik nr **PB -01**.

5. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, wzór wykazu stanowi załącznik nr **PB-02**

6. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

Opis struktury zbiorów danych dla poszczególnych programów przetwarzających dane osobowe – wzór stanowi załącznik nr **PB-03**.

7. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

Sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe – wzór stanowi załącznik nr **PB-04**

8. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

A) Zabezpieczenia organizacyjne:

1. został wyznaczony Inspektor Ochrony Danych Osobowych nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych (Zarządzenie z dnia 25.05.2018r.) ,
2. została opracowana i wdrożona Polityka Bezpieczeństwa (niniejsze Zarządzenie z dnia 25.05.2018r.),
3. została opracowana i wdrożona instrukcja zarządzania systemem informatycznym (Zarządzenie z dnia 25.05.2018r.),
4. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora Danych Osobowych – wzór upoważnienia stanowi załącznik **PB-05**,
5. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych – wzór ewidencji stanowi załącznik **PB-06**,
6. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego – wzór dokumentu stanowi załącznik **PB-06**,
7. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy – wzór oświadczenia zawarty w załącznik **PB-05**,
8. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
9. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
10. ustalono rejestr czynności przetwarzania – według wzoru stanowiącego załącznik **nr PB-14** - wprowadzony Zarządzeniem z dnia 25.05.2018 r.
11. ustalono rejestr kategorii przetwarzania stosowany u podmiotów przetwarzających, z którymi Administrator zawiera stosowne umowy – według wzoru stanowiącego załącznik **PB – 15;**

12. ustalono wzory wniosków obejmujących: dostęp do danych (art. 15 ogólnego rozporządzenia RODO), sprostowania danych (art. 16 ogólnego rozporządzenia RODO); usunięcia danych (art. 17 ogólnego rozporządzenia RODO), ograniczania przetwarzania (art. 18 ogólnego rozporządzenia RODO), przenoszenie danych (art. 20 ogólnego rozporządzenia RODO) – zgodnie z wzorem stanowiącym załącznik nr **PB - 16**
13. określono wzór zgłoszenia naruszenia danych osobowych oraz wzór zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony jej danych osobowych – według wzoru n**r PB - 17**
14. określono wzór **rejestru dla oceny skutków dla ochrony** danych jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – stanowiący załącznik nr **PB -18**
15. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe – według wzoru stanowiącego załącznik nr **PB-12**
16. **stosuje się pisemne zgody na przetwarzania danych osobowych – według wzoru stanowiącego załącznik nr PB-13**
17. Procedurę określającą zasady dostępu do pomieszczeń w którym przetwarzane są dane osobowe określa załącznik nr **PB-19**

B) Zabezpieczenia ochrony fizycznej danych osobowych:

1. wyznaczono adekwatne do zagrożeń zabezpieczenia i zaznaczono je na liście zabezpieczeń zbiorów i programów – wzór stanowi załącznik nr **PB-02.**

C) Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

1. wyznaczono adekwatne do zagrożeń zabezpieczenia i zaznaczono je na liście zabezpieczeń zbiorów i programów – wzór stanowi załącznik nr **PB-02.**

D) Zabezpieczenia narzędzi programowych i baz danych:

1. wyznaczono adekwatne do zagrożeń zabezpieczenia i zaznaczono je na liście zabezpieczeń zbiorów i programów – wzór stanowi załącznik nr **PB-02.**

9. INSTRUKCJA ALARMOWA

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości. Wzór instrukcji stanowi załącznik nr **PB-07**.

10. PROCEDURA DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH

Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych.– wzór procedury stanowi załącznik nr **PB-08**.

11. PROCEDURA KONTROLI SYSTEMU OCHRONY DANYCH OSOBOWYCH

Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: kontrolą stanu bezpieczeństwa danych osobowych.– wzór procedury stanowi załącznik nr **PB-09**.

12. PROCEDURA REKRUTACJI.

Procedura opisuje zasady podczas prowadzenia procesu rekrutacji nowych pracowników, dane które należy zbierać oraz klauzule które mają być zawarte w dokumentacji aplikacyjnej. – wzór procedury stanowi załącznik nr **PB-20**.

13. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH.

Procedura opisuje zasady: nadawania upoważnień do przetwarzania zbiorów danych osobowych oraz do zarządzania uprawnieniami użytkowników w systemie informatycznym lub w wersji papierowej. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty poufności przez osoby nieupoważnione. – wzór procedury stanowi załącznik nr **PB-21.**

14. PROCEDURA DOSTĘPU PODMIOTÓW ZEWNĘTRZNYCH

Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa Administrator Danych Osobowych i. – wzór procedury stanowi załącznik **PB-22.**

15. SPRAWOZDANIE ROCZNE STANU SYSTEMU OCHRONY DANYCH OSOBOWYCH

1. Raz w roku Inspektor Ochrony Danych Osobowych przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych

2. W spotkaniu sprawozdawczym uczestniczą: IODO , Kierownicy działów, w których przetwarzane są dane osobowe, Informatyk.

3. Raport przygotowany jest według wzoru załącznika **PB-10** a następnie przedstawiany jest Administratorowi Danych Osobowych.

16. SZKOLENIA UŻYTKOWNIKÓW

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu lub zapoznany z polityką/regulaminem ochrony danych osobowych/ instrukcją zarządzania systemem informatycznym.

2. Za przeprowadzenie szkolenia lub zapoznania polityką/regulaminem ochrony danych osobowych/instrukcją zarządzania systemem informatycznym odpowiada IODO.

3. Zakres szkolenia/zaznajomienia powinien obejmować przepisy ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi, rozporządzeniem PEiRUE oraz dokumentację ochrony danych osobowych, obowiązującą u Administratora Danych Osobowych, a także zobowiązanie się do ich przestrzegania.

4. Po szkoleniu lub po zapoznaniu się z polityką/regulaminem ochrony danych osobowych/ instrukcją zarządzania systemem informatycznym, użytkownik zobowiązany jest do podpisania Oświadczenia o poufności.

5. Odbycie szkolenia (od momentu planowania do momentu przeprowadzenia) jest rejestrowane według wzoru załącznika **PB-11**.

17. POSTANOWIENIA KOŃCOWE

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

2. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią Polityki Bezpieczeństwa każdego użytkownika.

3. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa.

5. W przypadku wystąpienia sytuacji, w której dany załącznik Polityki Bezpieczeństwa bądź Instrukcji zarządzania systemami informatycznymi, nie będzie konieczny do wykorzystania na daną chwilę w jednostce, należy go traktować jako załącznik z możliwością wdrożenia w przyszłości.

6. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

7. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

8. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. 2016 r. poz. 922 ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

9. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922 ze zm.) oraz wydanych na jej podstawie aktów wykonawczych oraz rozporządzenie RODO.

WÓJT
mgr inż. Barbara Dybczak

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-01

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

	Adres	Pokój	Zabezpieczenia	Data zakończenia przetwarzania
1				
2				
3				
4				
5				
6				
7				

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-02

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

	Nazwa zbioru danych osobowych	Nazwy Programów	Zabezpieczenia	Opis zbioru
1				
2				
3				
4				
5				
6				
7				

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-03

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

	Nazwa zbioru danych osobowych	Opis struktury
1		
2		
3		
4		
5		
6		
7		

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-04

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

(forma tabeli bądź schematu)

System (Moduł) A	System (Moduł) B	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-05

……, dnia .....

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym upoważniam
Imię i Nazwisko , nr PESEL .....

do przetwarzania danych osobowych w niżej określonym zakresie:

L.p.	Nazwa bazy danych	Wprowadzanie	Przeglądanie	Aktualizacja	Udostępnianie	Usuwanie
1.	PRACOWNICY	☐	☐	☐	☐	☐
2.		☐	☐	☐	☐	☐
3.		☐	☐	☐	☐	☐
4.		☐	☐	☐	☐	☐

LUB

do przetwarzania danych osobowych w systemie tradycyjnym oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w Urzędzie ……., a w szczególności do danych osobowych zawartych w zbiorach danych:

.....

.....

Identyfikator: .....
(Wypełnia się w przypadku , gdy dane przetwarzane są w systemie informatycznym)

Powyższe upoważnienie jest ważne na czas trwania zatrudnienia w Urzędzie ..... lub do pisemnego odwołania.

.....

Z upoważnienia Administratora Danych Osobowych

Oświadczenie osoby upoważnianej

Ja, niżej podpisany(a) *Imię i Nazwisko* oświadczam, że zobowiązuję się do zachowania poufności danych objętych niniejszym upoważnieniem oraz sposobów ich ochrony zarówno w trakcie jego ważności, jak i po jej ustaniu. Oświadczam jednocześnie, że zostałem(am) przeszkolony(a) w zakresie przepisów regulujących przetwarzanie danych osobowych oraz Polityki bezpieczeństwa, obowiązującej w *Urzędzie ... .*

.....

Data i własnoręczny podpis

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-06

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Oświadczam, że zapoznałem/łam się z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym w .....:

Imię i nazwisko	**Funkcja**	**Data nadania uprawnień**	**Data ustania uprawnień**	**Zakres upoważnienia**	**ID***	**Podpis osoby upoważnionej**

**dotyczy, gdy osoba przetwarza dane osobowe w systemie informatycznym*

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-07

INSTRUKCJA ALARMOWA

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub IODO.

2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia zagrożenia, IODO prowadzi postępowanie wyjaśniające w toku, którego:

a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
b. inicjuje ewentualne działania dyscyplinarne,
c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
d. dokumentuje prowadzone postępowania.

5. W przypadku stwierdzenia incydentu (naruszenia), IODO prowadzi postępowanie wyjaśniające w toku, którego:

a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały
b. zabezpiecza ewentualne dowody

c. ustala osoby odpowiedzialne za naruszenie
d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody)
e. inicjuje działania dyscyplinarne
f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości
g. dokumentuje prowadzone postępowania

6. Do rejestracji incydentów i niezgodności służy załącznik **PB-07A.**

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-07a

DZIENNIK REJESTRACJI INCYDENTÓW

L.p.	Data	Typ	Nazwa	Osoba zgłaszająca	Uwagi (status/rozwiązanie)

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-08

PROCEDURA DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych.

2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami stawy o Ochronie Danych Osobowych, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.

3. Osobą odpowiedzialną za nadzór nad procedurą jest IODO.

Definicje

1. Incydent - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
2. Zagrożenie – potencjalna możliwość wystąpienia incydentu
3. Korekcja – działanie w celu wyeliminowania skutków incydentu.
4. Działanie korygujące – jest to działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji.
5. Działanie zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.
6. Kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki i instrukcji.

Opis czynności

1. IODO jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:

- zgłoszenia od pracowników
- wiedza IODO
- wyniki kontroli

2. W przypadku, gdy IODO stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną

3. IODO jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.

4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, IODO jest zobowiązany do oceny efektywności ich zastosowania.

5. Do rejestracji działań korygujących i zapobiegawczych załącznik **PB-08A**

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-08a

DZIENNIK DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH

L.p.	Data	Typ	Nazwa	Źródło	Uwagi (status/rozwiązanie)

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-09

PROCEDURA KONTROLI SYSTEMU OCHRONY DANYCH OSOBOWYCH

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: kontrolą stanu bezpieczeństwa danych osobowych

2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.

3. Do kontroli stanu ochrony danych osobowych upoważniony jest wyznaczony kontroler wewnętrzny np. ASI oraz kierownik danej jednostki - ADO.

4. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami U.O.D.O.

5. IODO przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.

6. Kontrola przeprowadzana jest na podstawie listy kontrolnej dokumentu załącznik **PB-09A** - lista kontrolna ODO

7. Po dokonanej kontroli osoba ją przeprowadzająca przygotowuje i przekazuje raport pokontrolny (załącznik **PB-09B** – Raport pokontrolny) kierownikowi kontrolowanej jednostki lub komórki organizacyjnej oraz Administratorowi Danych Osobowych. Na jego podstawie IODO inicjuje działania korygujące lub zapobiegawcze.

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-09A

LISTA KONTROLNA ODO

Jednostka audytowana				.....
Nazwa zadania audytowego				Audyt bezpieczeństwa informacji
Lp.	Pytanie	Odpowiedź		Uwagi/uzasadnienie
		TAK	NIE	
Polityka bezpieczeństwa				
	Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.			
	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.			
	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.			
	Sposób przepływu danych pomiędzy poszczególnymi systemami.			
	Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.			
Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych				
	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.			
	Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i			

	użytkowaniem.			
	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.			
	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.			
	Sposób, miejsce i okres przechowywania: • elektronicznych nośników informacji zawierających dane osobowe; • kopii zapasowych.			
	Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia. (System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed: 1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego)			
	Czy system informatyczny zapewnia odnotowanie daty wprowadzenia: • danych do systemu • identyfikatora wprowadzającego • źródła danych gdy zbierane dane nie od osoby której dotyczą Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 (odnotowanie informacji o odbiorcach, którym zostały udostępnione dane osobowe).			
	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.			

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-09b

RAPORT POKONTROLNY

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-10

SPRAWOZDANIE ROCZNE STANU SYSTEMU OCHRONY DANYCH OSOBOWYCH

ZAŁĄCZNIK do polityki bezpieczeństwa-PB-11

SZKOLENIA UŻYTKOWNIKÓW

L.p.	Data	Osoba szkoląca	Temat Szkolenia	Osoba uczestniczące	Podpis osób uczestniczących

ZAŁĄCZNIK PB-12 do Polityki Bezpieczeństwa

Umowa
powierzenia przetwarzania danych osobowych

zawarta w dniu ..... w ....., pomiędzy:

..... reprezentowaną przez
.....

zwaną dalej „**Administratorem**"

a

.....

.....

zwanym dalej **„Przetwarzającym"**

(dalej łącznie jako: „**Strony**")

Mając na uwadze, że:

Strony zawarły umowę ..... („**Umowa Podstawowa**"), w związku, z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową;

Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;

Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO**.

Opis Przetwarzania

Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.

Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.

Charakter i cel przetwarzania wynikają z Umowy Podstawowej. W szczególności dotyczą powierzeniu przez Administratora danych osobowych, które będą przetwarzane przez Przetwarzającego wyłączenie w celu realizacji umowy .....

Przetwarzanie obejmować będzie następujące rodzaje danych osobowych („**Dane**"):

Dane zwykłe:

imię i nazwisko,

adres zamieszkania,

numery telefonów,

.....

Przetwarzanie Danych będzie dotyczyć następującej kategorii osób: ..... oraz innych podmiotów (osób trzecich), jeśli będzie konieczne.

Podpowierzenie

Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („**podpowierzenie**") w drodze pisemnej umowy podpowierzenia („**Umowa Podpowierzenia**") innym podmiotom przetwarzającym. („**Podprzetwarzający**"), pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.

Lista Podprzetwarzających zaakceptowanych przez Administratora stanowić będzie **Załącznik do Umowy podpowierzenia – Lista Zaakceptowanych Podprzetwarzających**.

Sprzeciw. Powierzenie przetwarzania Danych Podprzetwarzającym spoza Listy Zaakceptowanych Podprzetwarzających wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia Danych konkretnemu Podprzetwarzającemu. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć Danych Podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego Podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu Podprzetwarzającemu. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

Dokonując podpowierzenia Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.

Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy.

Przetwarzający ma następujące obowiązki:

Przetwarzający przetwarza Dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

Przetwarzający oświadcza, że nie przekazuje Danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy („**EOG**")). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.

Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać Dane poza EOG, informuje o tym Administratora, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.

Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

Przetwarzający zapewnia ochronę Danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.

Przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (Podprzetwarzającego).

Przetwarzający w miarę możliwości pomaga Administratorowi z pomocą środków technicznych i organizacyjnych do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO („**Prawa jednostki**").

Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z

obszaru ochrony danych osobowych, o których mowa w art. 32–36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

Planując dokonanie zmian w sposobie przetwarzania Danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Przetwarzającego.

Przetwarzający zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do Danych jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.

Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru czynności przetwarzania danych osobowych (wymóg art. 30 RODO). Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.

Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

Obowiązki Administratora

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

Bezpieczeństwo danych

Administrator i podmiot przetwarzający wdrożą odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa w ochronie danych osobowych, odpowiadający temu ryzyku.

Powiadomienie o Naruszeniach Danych Osobowych

Przetwarzający powiadamia Administratora danych o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.

Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.

Nadzór

Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim

poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do (i) wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz (ii) wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.

Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

Przetwarzający w okresie trwania umowy:

(1) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,

(2) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

Oświadczenia Stron

Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.

Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętych Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

Odpowiedzialność

Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego.

Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

Umowa została zawarta na czas obowiązywania Umowy Podstawowej.

Usunięcie Danych

Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych i jest zobowiązany do:

(1) usunięcia Danych,

(2) usunięcia wszelkich ich istniejących kopii lub zwrotu Danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie Danych.

(3) Strony uzgodnią sposób usunięcia Danych odrębnym dokumentem w ciągu 30 dni od zawarcia Umowy Powierzenia.

Przetwarzający dokona usunięcia Danych po upływie 180 dni od zakończenia Umowy, chyba że Administrator poleci mu to uczynić wcześniej.

Po wykonaniu zobowiązania, o którym mowa wyżej, Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich Danych.

Postanowienia Końcowe

W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy Powierzenia a Umowy

Podstawowej, pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Umowa podlega prawu polskiemu oraz RODO.

Administrator

Przetwarzający

Załącznik PB - 13 do Polityki Bezpieczeństwa

Wyrażam zgodę na przetwarzanie danych osobowych zgodnie z przepisami ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. oraz ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. ….. r. poz. …...) przez ……. z siedzibą w ……., ul. ……., dla celów związanych z ……..
Wyrażam również zgodę na przekazanie moich danych …… i ewentualną weryfikację prawdziwości przekazanych przeze mnie dokumentów i zawartych w nich informacji.
Jednocześnie oświadczam, iż świadomie i dobrowolnie wyrażam zgodę na udostępnianie podanych przeze mnie danych dla potrzeb …… z siedzibą w …….. oraz posiadam wiedzę na temat celu zbierania danych, znanych oraz przewidywanych odbiorcach i kategoriach odbiorców danych i przysługujących mi praw do wglądu, uzupełniania, poprawiania oraz żądania usunięcia moich danych.

KLAUZULA INFORMACYJNA – WZÓR OGÓLNY
Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1) administratorem Pani/Pana danych osobowych jest … (nazwa ADO*) z siedzibą w … (**adres*) (**dodatkowo należy podać dane przedstawiciela jeżeli istnieje*);**
2) inspektorem ochrony danych w … (nazwa ADO*) jest Pan/Pani (**imię i nazwisko inspektora*) … (**e-mail lub inne dane kontaktowe*) … ;**
3) Pani/Pana dane osobowe przetwarzane będą w celu … (należy podać cel przetwarzania*) na podstawie … (**należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f. *Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej*);**
4) odbiorcą Pani/Pana danych osobowych będą … (można wymienić kategorię odbiorców o ile istnieją*);**
5) Pani/Pana dane osobowe będą przechowywane przez okres … *(*jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięscy konkursu, do czasu zakończenia rekrutacji itd.)*;
6) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania *(*jeżeli przetwarzanie odbywa się na podstawie zgody)*, którego dokonano na podstawie zgody przed jej cofnięciem;
7) ma Pan/Pani prawo wniesienia skargi do UIODO gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;
8) podanie przez Pana/Panią danych osobowych jest … *(*wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy)*. Jest Pan/Pani zobowiązana do ich podania a konsekwencją niepodania danych osobowych będzie … *(* jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych)*;

	1	2	3	4	5	6	7	8	9
Lp.	Czynności przetwarzania danych osobowych	Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;	Cele przetwarzania;	Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;	Gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;	Jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;	Jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	Uwagi
1									
2									
3									
4									
5									

	1	2		3	4	5	6	7	8	9
Lp.	Kategorie czynności przetwarzania danych osobowych	Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;	Nazwa i dane Inspektora Ochrony Danych (IOD) administratora	Cele przetwarzania;	Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;	Gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;	Jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;	Jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	Uwagi
1										
2										

Załącznik PB-16

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do.....
(dokładne oznaczenie administratora danych)

2. Wnioskodawca.....
.....
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy,
ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych : *Na podstawie art. 15 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) wnoszę o udostępnienie danych osobowych:*

4. Wskazanie przeznaczenia dla udostępnionych danych:.....
.....
.....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:.....
.....

6. Zakres żądanych informacji ze zbioru:.....
.....
.....

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych:.....
.....
.....

podpis

Żądanie sprostowania danych osobowych

Ja niżej podpisana/y, (...), na podstawie art. 16 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), żądam sprostowania moich danych osobowych, tj. (...), przetwarzanych przez (...).

Uzasadnienie

W tym miejscu należy umieścić: - informację dotyczące przyczyn i zakresu danych, które są nieprawdziwe i wskazać (w razie potrzeby dołączyć) dowody uprawdopodabniające te okoliczności.

podpis

Żądanie usunięcia danych osobowych

Ja niżej podpisana/y, (...),na podstawie art. 17 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), żądam usunięcia moich danych osobowych, tj. (...), przetwarzanych przez (...).

Uzasadnienie

W tym miejscu należy umieścić: - informację dotyczące przyczyn i zakresu danych, które mają być usunięte i wskazać (w razie potrzeby dołączyć) dowody uprawdopodabniające te okoliczności.

podpis

Wniosek o przenoszenie danych osobowych

Ja niżej podpisana/y, (...),na podstawie art. 20 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), wnoszę o przeniesienie moich danych osobowych, tj. (...), przetwarzanych przez (...).

Uzasadnienie

W tym miejscu należy umieścić: - informację dotyczące przyczyn i zakresu danych, których przeniesienie ma dotyczyć i wskazać (w razie potrzeby dołączyć) dowody uprawdopodabniające te okoliczności.

podpis

Żądanie ograniczenia przetwarzania danych osobowych

Ja niżej podpisana/y, (...),na podstawie art. 18 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), żądam ograniczenia moich danych osobowych, tj. (...), przetwarzanych przez (...).

Uzasadnienie

W tym miejscu należy umieścić: - informację dotyczące przyczyn i zakresu danych, których ograniczenia przetwarzania dotyczy i wskazać (w razie potrzeby dołączyć) dowody uprawdopodabniające te okoliczności.

podpis

Załącznik PB-17 do Polityki Bezpieczeństwa

.....
(miejscowość, data)

Administrator danych
.....

UODO
.....

ZGŁOSZENIE
W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu … w … .

1.	**Charakter naruszenia ochrony danych:**	
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	
3.	**Liczba rekordów, których dotyczy naruszenie:**	
4.	**Możliwe konsekwencje naruszenia ochrony danych:**	
5.	**Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	

6.	**Dane inspektora ochrony danych***	

.....
.....
.....**

.....
(czytelny podpis administratora danych, zgodnie z reprezentacją podmiotu)

* W przypadku niepowołania należy wskazać inny punkt kontaktowy.
**W przypadku zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin, administrator danych zobowiązany jest do złożenia wyjaśnień w przedmiocie przyczyn opóźnienia.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

Zawiadomienie, jasnym i prostym językiem powinno opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej niżej wymienione informacje:

1. Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji.

2. Opisywać możliwe konsekwencje naruszenia ochrony danych osobowych.

3. Opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie nie jest wymagane w następujących przypadkach:

1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.
2. administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt. 1.
3. Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, wymienionych wyżej.

Załącznik PB-18 do Polityki Bezpieczeństwa

Rejestr dla oceny skutków dla ochrony danych

L.p.	Opis planowanych operacji przetwarzania	Ocena czy operacje przetwarzania są niezbędne oraz proporcjonalne	Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą	Środki planowane w celu: - zaradzenia ryzyku i przestrzegania rozporządzenia

ZAŁĄCZNIK PB-19 do polityki bezpieczeństwa

Polityka kluczy i dostępu do pomieszczeń w których przetwarzane są dane osobowe

1. Ogólne zasady

a. Polityka kluczy obejmuje pomieszczenia przy ulicy .....
b. Obowiązuje pięciodniowy tydzień pracy, tzn. od poniedziałku do piątku, w godzinach ..... – .....
c. Dostęp do pomieszczeń biurowych możliwy jest wyłącznie poprzez wyznaczone do tego drzwi. Wszystkie pozostałe drzwi umożliwiające dostęp do pomieszczeń biurowych powinny być trwale zamknięte na klucz. Zabrania się otwierania tych drzwi przez pracowników bez zgody AOD.
d. Klucze zapasowe przechowywane są w portierni / sejfie / podać inne miejsce.

2. Nadawanie upoważnień

a. Upoważnienia do pobierania kluczy do pomieszczeń mają wyłącznie osoby upoważnione przez kierowników jednostek. Obejmują one także dostęp do biura poza godzinami pracy.
b. Udzielenie/anulowanie upoważnienia wymaga wprowadzenia osoby do ewidencji, prowadzonej w postaci załącznika **PB-19A** - Ewidencja dostępu do pomieszczeń.

3. Wydawanie i zdawanie kluczy w trybie normalnym

a. Klucze do budynku wydawane są za pobraniem przez (np. portiernię, sekretariat) / Klucze do budynku pozostają pod osobistym nadzorem osób upoważnionych.
b. Klucze do pomieszczeń wydawane są za pobraniem przez (np. portiernię, sekretariat) / Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych.
c. Klucze do pomieszczeń szczególnie chronionych (np. serwerowni) wydawane są za pobraniem przez (np. portiernię, sekretariat) / Klucze do pomieszczeń szczególnie chronionych (np. serwerowni) pozostają pod osobistym nadzorem osób upoważnionych. Dostęp do tych pomieszczeń osób trzecich odbywa się pod ścisłym nadzorem!.
d. Pracownicy upoważnieni zobowiązani są do odnotowania pobrania i zdania kluczy – załącznik **PB-19B** Ewidencja pobrań.

4. Wydawanie i zdawanie kluczy w trybie nadzwyczajnym

a. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą bezpośredniego przełożonego.
b. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu za poświadczeniem zwrotu w Ewidencji dostępu do pomieszczeń.

5. Bieżące postępowanie w trakcie dnia pracy

a. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
b. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
c. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
d. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w specjalnej skrytce / szufladzie / biurku / podać inne miejsce. Klucz zbiorczy jest zabezpieczony w portierni / sejfie / podać inne miejsce

e. Po zakończeniu pracy, pracownicy są zobowiązani do:
   - wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych
   - wyłączenia oświetlenia,
   - zabezpieczenia i zamknięcia okien i drzwi
   - ew. aktywacji alarmu
   - usunięcia dokumentów i treści zawierających dane osobowe z biurek, szafek i schowanie ich do szaf/biurek, a następnie ich zamknięcie, i pochowanie kluczy do tych szaf
   - zamknięcia wszystkich pomieszczeń i oddanie kluczy

f. Za przestrzeganie w/w zasad bieżących odpowiada kierownik podległej jednostki.

g. W trakcie pracy pracownik obsługujący klientów, prowadzi obsługę w ten sposób aby rozmowy o danych osobowych były prowadzone indywidualnie, odrębnie od innych, przy stoliku z dala od miejsca, gdzie dany pracownik pracuje na danych osobowych innej osoby.

6. Sankcje. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie następujących konsekwencji:

a. poniesienie odpowiedzialności wynikających z art. 52 kodeksu pracy,
b. poniesienie odpowiedzialności wynikających z art. 363 § 1. kodeksu cywilnego.

ZAŁĄCZNIK PB-19A do Polityki Bezpieczeństwa

EWIDENCJA OSÓB MAJĄCYCH DOSTĘP DO POMIESZCZEŃ PRZETWARZANIA DANYCH

L.p.	Imię i Nazwisko	Data nadania dostępu	Data odebrania dostępu	Pomieszczenia	Podpis Osoby upoważnionej
1.					

ZAŁĄCZNIK PB-19B do Polityki Bezpieczeństwa

EWIDENCJA POBRAŃ KLUCZY DO POMIESZCZEŃ POD ŚCISŁYM NADZOREM

L.p.	Imię i Nazwisko	Data pobrania kluczy	Data oddania kluczy	Pomieszczenia	Podpis Osoby pobierającej
1.					

ZAŁĄCZNIK PB-20 do Polityki Bezpieczeństwa

PROCEDURA REKRUTACJI PRACOWNIKÓW

1. Celem procedury jest ustalenie zasad stosowanych w .....

2. Osobą odpowiedzialną za nadzór nad procedurą jest ADO.

Opis czynności

1. Przed przystąpieniem do rekrutacji należy określić zakres danych który będzie niezbędny w trakcie tego procesu i nie będzie zawierał danych ponad te określone w art. 22^1 § 1 Kodeksu pracy.

- imię (imiona),
- nazwisko,
- imiona rodziców,
- datę urodzenia,
- miejsce zamieszkania (adres do korespondencji),
- wykształcenie,
- przebieg dotychczasowego zatrudnienia,
- innych danych niż wyżej wymienione można wymagać wyłącznie w przypadku, gdy obowiązek ich podania wynika z odrębnych przepisów.

2. Każda przesłana aplikacja powinna być opatrzona zgodą w formie:

„Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w ofercie pracy dla potrzeb procesu rekrutacji zgodnie z ustawą z dnia 29.08.1997 r. o Ochronie Danych Osobowych, tekst jednolity: Dz. U. ..... r. poz. ..... z późn. zm."

oraz opatrzona odręcznym podpisem.

3. Brak załączonej zgody na przetwarzanie danych osobowych traktowany jest jako brak formalny.
Oznacza to, że rekruter nie może włączyć zgłoszonego CV do procesu rekrutacji. Dlatego bez takiego pozwolenia np. nie może zaprosić kandydata na rozmowę kwalifikacyjną, która jest kolejnym etapem rekrutacji. Co do zasady, dokumenty aplikacyjne bez załączonej zgody należy usunąć z procesu rekrutacji. Jednak, gdy kandydat skontaktuje się rekruterem w celu poznania powodów odrzucenia jego aplikacji, może uzupełnić ten brak formalny.

4. Dane aplikacyjne jako zbiór danych osobowych nie jest zgłaszany do UIODO lecz spełniane są wszelkie wymagania dotyczące ochrony danych osobowych.

5. Dokumenty rekrutacyjne należy zniszczyć do 180 dni od czasu rekrutacji wg procedury **IZSI-06A**.

ZAŁĄCZNIK PB-21 do Polityki bezpieczeństwa

PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

Procedura opisuje zasady: nadawania upoważnień do przetwarzania zbiorów danych osobowych oraz do zarządzania uprawnieniami użytkowników w systemie informatycznym lub w wersji papierowej. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty poufności przez osoby nieupoważnione.

1. Nadawanie upoważnień do przetwarzania danych osobowych i zarządzanie uprawnieniami użytkowników.

   a. Imienne upoważnienie do przetwarzania danych osobowych nadaje ADO - zgodnie z zakresem obowiązków .
   b. ADO przed nadaniem upoważnienia odpowiada za przeszkolenie (przeszkolenie w porozumieniu z IODO) osoby upoważnionej z zasad przestrzegania bezpieczeństwa danych osobowych.
   c. ADO odpowiada za uzyskanie od osoby upoważnionej oświadczenia o poufności.
   d. ADO zleca nadanie identyfikatora osobie upoważnionej (użytkownikowi) w systemie informatycznym Administratorowi Systemu Informatycznego. (załącznik **PB-21A**)
   e. ADO odpowiada za wycofanie upoważnień i zmianę zakresu uprawnień dla użytkowników.
   f. Usunięcie uprawnień użytkownikowi polega na wyrejestrowaniu go z systemu przez Informatyka (ASI) na zlecenie ADO.
   g. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
   h. ADO odpowiada za formalne dokumentowanie Upoważnień/Oświadczeń w aktach osobowych pracowników. Realizuje to w załączniku **PB-06 do Polityki Bezpieczeństwa.**
   i. ADO opowiada za prowadzenie Ewidencji osób upoważnionych do przetwarzania Danych Osobowych. Realizuje to według wzoru określonego w załączniku **PB-06 do Polityki Bezpieczeństwa.**

2. Zarządzanie uprawnieniami administratorów

   a. Administratorów Systemów Informatycznych (tzw. Użytkowników uprzywilejowanych) powołuje pisemnie Administrator Danych Osobowych na podstawie zarządzenia.
   b. Każdy Administrator Systemu Informatycznego zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta „root" / „administrator", dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.

ZAŁĄCZNIK PB-21A do Polityki Bezpieczeństwa

WNIOSEK O UDZIELENIE / ODEBRANIE / ZMIANĘ DOSTĘPU DO ZASOBU INFORMATYCZNEGO

....., dnia .....

.....
Jednostka Organizacyjna/Symbol komórki org.

.....
Imię i nazwisko pracownika/nr kadrowy lub nazwa podmiotu zewnętrznego oraz imię i nazwisko osoby ubiegającej się o dostęp

Numer telefonu kontaktowego: .....

PROSZĘ O UDZIELENIE/ODEBRANIE/ZMIANĘ[1] DOSTĘPU DO ZASOBÓW:

☐ **Konto - logowanie do komputera**

- utworzenie/odblokowanie/zablokowanie konta[1]

☐ **Poczta elektroniczna e-mail**

- utworzenie/usunięcie/zablokowanie[1] konta
- włączenie/wyłączenie[1] synchronizacji poczty służbowej z urządzeniem mobilnym

☐ **Nazwa Zasobu Informatycznego:**

.....

.....

Uzasadnienie: .....

.....

Uwagi: .....

Zgoda Właściciela:

.....

podpis i pieczątka osoby wnioskującej

.....

data, podpis i pieczątka

---

[1] niepotrzebne skreślić

ZAŁĄCZNIK PB- 22 do Polityki Bezpieczeństwa

PROCEDURA DOSTĘPU PODMIOTÓW ZEWNĘTRZNYCH

Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa Administrator Danych Osobowych.

2. Administrator Danych powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o umowę powierzenia przetwarzania danych (załącznik **PB-20**).

a. Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia przetwarzania danych osobowych.
b. Podmiot zewnętrzny zobowiązany jest do stosowania zabezpieczeń określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).
c. Podmiot przetwarzający zobowiązany jest do przetwarzania danych zgodnie z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
d. Podmiot przetwarzający zobowiązany jest do prowadzenia rejestru kategorii czynności przetwarzania – zgodnie z ww. Rozporządzeniem

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Urząd Gminy w Skoroszycach

Spis treści

1. WSTĘP

Instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych.

Instrukcję opracowana na podstawie:

1) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 ze zm.)
2) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).,
3) wewnętrznego regulaminu ochrony danych osobowych,
4) spełnienia kryteriów określonych w § 6 ust. 1 pkt 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (rozporządzenie PEiRUE), dalej zwanym „rozporządzeniem RODO" i w części C załącznika do tego Rozporządzenia, tj. zabezpieczenia na poziomie wysokim.

Dla każdej osoby, której dane osobowe przetwarzane są w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępniania go na piśmie – system ten winien zapewniać odnotowanie:

1. daty pierwszego wprowadzenia danych do systemu,
2. identyfikatora wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada jedna osoba,
3. źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą,
4. informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny jest używany do przetwarzania danych zawartych w zbiorach jawnych,
5. sprzeciwu wobec przetwarzania jej danych, w przypadkach gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Odnotowanie informacji, o których mowa w pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt (1-5).

2. DEFINICJE

ASI – Administrator Systemu Informatycznego. Może nim być Informatyk zatrudniony na umowę o pracę lub zewnętrzna firma informatyczna.

3. PROCEDURA KORZYSTANIA Z INTERNETU

Celem procedury jest zapewnienie bezpiecznego korzystania z dostępu do internetu i zawiera się w załączniku **IZSI-01**.

4. PROCEDURA KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

Celem procedury jest określenie bezpiecznych zasad korzystania z poczty elektronicznej i zawiera się w załączniku **IZSI-02**.

5. METODY I ŚRODKI UWIERZYTELNIENIA

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione. Zasady opisano w załączniku **IZSI-03**.

6. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe. Zasady opisano w załączniku **IZSI-04**.

7. PROCEDURA TWORZENIA KOPII ZAPASOWYCH

Celem procedury jest zabezpieczenie danych osobowych przed zniszczeniem systemu informatycznego lub utratą danych osobowych mogącego nastąpić w skutek różnych zagrożeń powodujących zniszczenie lub zmienienie danych osobowych. Procedurę opisano w załączniku **IZSI-05**.

8. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI I WYDRUKÓW

Procedura określa sposób postępowania z nośnikami: twardymi dyskami, płytami CD/DVD, pendrive'ami, telefonami komórkowymi, pamięciami typu „flash" na których znajdują się dane osobowe, celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych. Zasady opisano w załączniku **IZSI-06**.

9. PROCEDURA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO, W TYM PRZED WIRUSAMI KOMPUTEROWYMI

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe. Zasady opisano w załączniku **IZSI-07**.

10. ZASADY I SPOSÓB ODNOTOWYWANIA W SYSTEMIE INFORMACJI O UDOSTĘPNIENIU DANYCH OSOBOWYCH

Celem procedury jest określenie zasad i sposobów odnotowania informacji o udostepnieniu danych osobowych które zostały określone w załączniku **IZSI-08**.

11. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem. Opis procedury zawiera załącznik **IZSI-09**.

WÓJT
mgr inż. Barbara Dybczak

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-01

PROCEDURA KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą ADO bądź ASI i tylko w uzasadnionych przypadkach.

Zabrania się korzystania z internetu lub z oprogramowania niezainstalowanego przez ASI lub za zgodą ADO na komputerze na którym zainstalowano oprogramowanie służące przetwarzaniu danych osobowych obejmujących systemy w zakresie ewidencji ludności, dowodów osobistych, danych stanu cywilnego i danych podatkowych.

3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu i przez niego zainstalowane.

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy sprawdzić, czy połączenie jest właściwie zabezpieczone. (ikonka „kłódki" podczas połączenia, adres internetowy powinien zaczynać się od słowa „https").

7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

Należy pamiętać, że nikt nie jest w sieci anonimowy, a korzystanie z każdej strony www jest utrwalane i może być wykorzystywane przez różne podmioty dla celów często niezgodnych z prawem.

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-02

PROCEDURA KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie informacji poza jednostkę może odbywać się tylko przez osoby do tego upoważnione.

2. W przypadku przesyłania informacji wrażliwych wewnątrz jednostki bądź wszelkich danych osobowych poza jednostkę należy wykorzystywać mechanizmy kryptograficzne (pakowanie i hasłowanie wysyłanych plików, podpis elektroniczny).

3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

4. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

5. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.

6. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia" itp.

7. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-03

PROCEDURA METOD I ŚRODKÓW UWIERZYTELNIENIA

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

Aby zachować bezpieczeństwo i zapobiec przetwarzaniu niezgodnemu z ogólnym rozporządzeniem o ochronie danych (RODO), ADO lub podmiot przetwarzający powinien oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej, a także koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie.

1. Ogólne zasady postępowania z hasłami

   a. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
   b. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
   c. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
   d. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła, gdy zostało ono ujawnione.
   e. Hasła do komputera oraz do poszczególnych programów powinny być zmieniane nie rzadziej niże raz na miesiąc

1. Hasła administratora

   a. Hasło administratora składa się co najmniej z 8 znaków.
   b. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
   c. Administrator systemu zobowiązany jest zmieniać swoje hasło nie rzadziej niż co 30 dni.
   d. Administrator zobowiązany jest do przechowywania haseł administratora w sejfie pod nadzorem Najwyższego Kierownictwa / utrzymywania równoległych kont i haseł administracyjnych dla co najmniej 2 administratorów.
   e. W przypadku utraty uprawnień przez osobę administrującą systemem, należy niezwłocznie zmienić hasła, do których miała dostęp.

2. Hasła do sieci i serwera – określamy, gdy na serwerze znajdują się dane osobowe.

   a. Hasło dostępu składa się co najmniej z 8 dla poziomu bezpieczeństwa wysokiego.
   b. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
   c. Zmiana hasła odbywa się co najmniej raz na 30 dni i jest wymuszana przez system / przez użytkowników.

3. Hasła do systemów przetwarzających dane osobowe

   a. Hasło dostępu składa się co najmniej z 8 znaków – wybieramy w dla poziomu bezpieczeństwa wysokiego.
   b. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków .
   c. Zmiana hasła odbywa się co najmniej raz na 30 dni i jest wymuszana przez system / przez użytkowników .

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-04

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.

2. Użytkownik jest zobowiązany do powiadomienia ADO oraz IODO o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.

3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.

4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu.

5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.

6. Po zakończeniu pracy, użytkownik zobowiązany jest:

a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-05

PROCEDURA TWORZENIA KOPII ZAPASOWYCH

1. **Tworzenie kopii bezpieczeństwa**

   a. Kopie zapasowe danych (np. kadrowo-płacowych) tworzone są przez użytkownika.
   b. Kopie całościowe sporządzane są raz w miesiącu a kopie przyrostowe raz dziennie.
   c. Kopie sporządzane są na płytach DVD (1 płyta miesięczna i 4 tygodniowe).
   d. Każda płyta jest opisana datą jej sporządzenia, etykietą nośnika, nr kolejnym, typem kopii, nazwą systemu informatycznego/ nazwą zbioru danych, identyfikator osoby wykonująca kopię . Wszystkie są zaewidencjonowane w „Rejestrze nośników komputerowych zawierających dane osobowe" stanowiącym załącznik **IZSI-05A** do niniejszej Instrukcji.
   e. Kopie całościowe przechowywane są przez 5 lat a kopie przyrostowe przez 1 miesiąc.
   f. Dostęp do kopii mają: ADO i Informatyka.
   g. Kopie przechowywane są w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu dyrekcji.
   h. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność wg załącznika **IZSI-05B**.
   i. Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.

2. **Tworzenie kopii bezpieczeństwa dokumentacji serwera**

   a. Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu o (specjalne oprogramowanie / wykorzystanie programowej funkcji serwera) * - wybrać opcję do tworzenia kopii bezpieczeństwa
   b. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym katalogu (np. w katalogu C:/Operacyjne/)
   c. Kopie całościowe sporządzane są raz w miesiącu a kopie przyrostowe raz dziennie
   d. Kopie sporządzane są na wydzielonym twardym dysku wymiennym na komputerze w pomieszczeniu recepcji.
   e. Dodatkowo – raz w miesiącu sporządzane są całościowe kopie miesięczne na streamerze
   f. Każda taśma streamera jest opisana datą jej sporządzenia
   g. Kopie całościowe przechowywane są przez okres 5 lat a kopie przyrostowe przez 1 miesiąc.
   h. Kopie przechowywane są w sejfie w pomieszczeniu szefa działu informatyki
   i. Dostęp do kopii mają: ADO i informatyka
   j. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność
   k. Niszczenie streamera odbywa się poprzez jego rozmontowanie i zniszczenie taśmy poprzez jej pocięcie

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM-IZSI-05A

REJESTR NOŚNIKÓW KOMPUTEROWYCH SŁUŻĄCYCH DO WYKONYWANIA KOPII ZAPASOWYCH

L.p.	Etykieta nośnika	Data wykonania kopii	Typ kopii	Nazwa systemu informatycznego/ zbór danych osobowych	Osoba wykonująca kopię
1.					

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM-IZSI-05B

RAPORT Z TESTU POPRAWNOŚCI KOPII ZAPASOWYCH

Lp.	Nazwa zasobu		Data testu	Wynik testu	Uwagi
1.					
	Opis testu (działań)				
2.					
	Opis testu (działań)				

Test przeprowadził:

.....

(Imię, nazwisko i podpis ASI)

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-06

PROCEDURA OKREŚLAJĄCA SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI I WYDRUKÓW

Procedura określa sposób postępowania z nośnikami: twardymi dyskami, płytami CD/DVD, pendrive'ami, telefonami komórkowymi, pamięciami typu „flash" na których znajdują się dane osobowe, celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

1. Zabezpieczenie elektronicznych nośników informacji

   a. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych.
   b. Zabrania się wynoszenia poza obszar jednostki wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody ADO.
   c. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:
      - adresat powinien zostać powiadomiony o przesyłce,
      - nadawca powinien sporządzić kopię przesyłanych danych,
      - dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
      - stosować bezpieczne koperty depozytowe,
      - przesyłkę należy przesyłać przez kuriera,
      - adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
   d. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).
   e. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny w/g załącznika **IZSI-06A**.
   f. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar jednostki (np. sprzedaż lub darowizna komputerów stacjonarnych / komputerów przenośnych).

2. Zabezpieczenie kopii zapasowych

Zabezpieczenie kopii zapasowych opisane jest w procedurach tworzenia kopii zapasowych.

3. Zabezpieczenie dokumentów i wydruków

a. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie zgodnie z zasadami określonymi w Polityce Bezpieczeństwa.
b. Za bezpieczeństwo dokumentów i wydruków odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych jednostek lub komórek organizacyjnych, a w szczególności odpowiadają za:
    - zamykanie dokumentów na klucz w szafach, biurkach, sejfach podczas nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. Polityka czystego biurka),
    - niszczenie dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania,
    - niepozostawianie wydruków i ksero na urządzeniach bez nadzoru.

4. Zabezpieczenie danych przesyłanych drogą elektroniczną.

Do zabezpieczenia danych przesyłanych drogą elektroniczną powyższe zasady stosuje się odpowiednio; w szczególności dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą. Zasady bezpieczeństwa określa **ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM.**

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-06A

PROCEDURA OKREŚLAJĄCA SPOSÓB NISZCZENIA NOŚNIKÓW Z DANYMI OSOBOWYMI

Procedura określa sposób postępowania w sytuacji niszczenia wszelkich nośników informacji zawierających dane osobowe lub licencjonowane oprogramowanie.

1. Procedura dotyczy Administratora Danych Osobowych i Administratora Systemu Informatycznego.
2. Tryb postępowania:
   a. Pod pojęciem nośnik informacji rozumiemy:
      - wydruki komputerowe,
      - dyski komputerowe,
      - płyty CD-R lub CD-RW,DVD,
      - taśmy magnetyczne,
      - dyskietki,
      - pamięci flash,
      - karty procesorowe.

   b. Procedura niszczenia dotyczy tych nośników informacji które zawierały bądź zawierają dane osobowe lub oprogramowanie podlegające licencjonowaniu.
   c. Przez niszczenie nośników rozumieć należy takie ich uszkodzenie mechaniczne, które uniemożliwia jakikolwiek odzysk zapisanych na nich informacji.
   d. Niszczeniu podlegają te nośniki, dla których minął okres ich ważności , nie przewiduje się ich dalszego użytkowania lub istnieje prawdopodobieństwo, że dalsze ich użytkowanie może nie spełniać przechowywania informacji.
   e. Niszczenie odbywa się na polecenie Administratora Systemu Informatycznego za wiedzą i zgodą ADO.
   f. Niszczenie dokonuje przynajmniej trzech pracowników na polecenie ASI.
   g. Niszczenie dokonuje się w sposób następujący:
      - wydruki papierowe czy foliowe niszczy się w niszczarce do papieru,
      - dyski twarde rozbiera się na części i niszczy talerze dysku,
      - płyty CD przełamuje się na kilka części lub korzysta z niszczarki,
      - taśmy magnetyczne wyciąga się z obudowy i przecina na części,
      - dyskietki przełamuje się na kilka części,
      - karty procesorowe przełamuje się, należy zwrócić uwagę aby zniszczyć procesor.
   h. Po zakończeniu niszczenia sporządzany jest rejestr likwidacji nośników stanowiący załącznik **IZSI-06B**.

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM-IZSI-06B

REJESTR ZNISZCZONYCH NOŚNIKÓW

L.p.	Etykieta nośnika	Data zniszczenia	Powód zniszczenia	Osoby niszczące nośnik	Podpisy
1.					

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-07

PROCEDURA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO, W TYM PRZED WIRUSAMI KOMPUTEROWYMI

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

1. Ochrona antywirusowa

   a. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
   b. System antywirusowy zainstalowano na serwerze oraz na stacjach roboczych
   c. System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej
   d. Użytkownicy zobowiązani są do skanowania plików programem antywirusowym.
   e. Zapewnia się stałą aktywność programu antywirusowego. Tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
   f. Aktualizacja definicji wirusów odbywa się automatycznie przez system
   g. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej.

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów

   a. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.
   b. Stosowany jest Firewall sprzętowy, programowy na serwerze, na stacjach roboczych
   c. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej
   d. Sieć bezprzewodową zabezpieczono technologią WPA2Personal
   e. Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one:
      - blokowanie stron internetowych określonego typu,
      - blokowanie określonych stron internetowych,
      - analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM -IZSI-08

PROCEDURA OKREŚLAJĄCA ZASADY I SPOSOBY ODNOTOWYWANIA W SYSTEMIE INFORMACJI O UDOSTĘPNIENIU DANYCH OSOBOWYCH

1. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:

   a. osoby, której dane dotyczą,
   b. osoby, upoważnionej do przetwarzania danych,
   c. administratora mającego siedzibę w państwie trzecim,
   d. podmiotu, któremu powierzono przetwarzanie danych,
   e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

2. System przetwarzający dane osobowe udostępniane odbiorcom musi umożliwiać rejestrację:

   a. nazwy jednostki organizacyjnej lub imienia i nazwiska osoby, której udostępniono dane,
   b. zakresu udostępnianych danych,
   c. daty udostępnienia.

3. Dane osobowe udostępnia się:

   a. osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
   b. pozostałym osobom lub podmiotom, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

4. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.

5. Zgody na udostępnienie danych udziela ADO.

6. Odnotowanie informacji o udostępnieniu danych powinno nastąpić niezwłocznie po udostępnieniu danych w systemie informatycznym przetwarzającym dane osobowe / w postaci ewidencji udostępniania stanowiącej załącznik **IZSI-08A**.

7. ADO odpowiada za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem.

8. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub wyciągu z rejestru papierowego, a raport przekazywany jest tej osobie.

ZAŁĄCZNIK do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM-IZSI-08A

EWIDENCJA UDOSTĘPNIENIA DANYCH OSOBOWYCH

L.p.	Nazwa jednostki której udostępniono dane osobowe	Data udostępnienia	Zakres danych udostępnionych	Podstawa	Podpis IODO
1.					

PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

1. Przeglądy i konserwacje systemu informatycznego i aplikacji.

   a. ASI odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.
   b. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku.
   c. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
   d. ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
   e. ASI odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, poczty email.
   f. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
   g. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
   h. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
   i. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren jednostki, należy:
      - wymontować nośniki z danymi osobowymi,
      - trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
      - nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.

2. Aktualizacje oprogramowania

   a. ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
   b. ASI odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

3. Dziennik administratora

   a. ASI dokumentuje pracę w załącznikach do Polityki Bezpieczeństwa **PZB-07A i PZB-08A**.